ABSTRACT

A method of production and distribution of asymetric public and private keys between a key generation centre and at least one user unit (DEC), the unit comprising a security module (SM), the method consisting in generating certificates comprising a public key and a private key in a first cryptographic unit (KPG), coding the private key by use of a service key in the first cryptographic unit (KPG) and storing the private key in a key memory (KPS), when sending the keys to a user unit, extracting the keys from the key memory (KPS), composing the certification with the public key, decoding the corresponding private key by use of the service key in a cryptographic security module and coding it with a transport key of the user.